Juridisk Publikation
STOCKHOLM - UPPSALA - LUND - GÖTEBORG - UMEÅ

Johan Kahn och Fredrik Gustafsson

Gemensamt personuppgiftsansvar – vanligare under GDPR?

Särtryck ur häfte 2/2017

Nummer 2/2017

GEMENSAMT PERSONUPPGIFTSANSVAR – VANLIGARE UNDER GDPR?

Av Johan Kahn och Fredrik Gustafsson[1]

Artikel 26 GDPR[2] och dess krav på ett "inbördes arrangemang" när flera aktörer är gemensamt personuppgiftsansvariga innebär enligt vår bedömning att det gemensamma personuppgiftsansvaret sannolikt kommer att få större betydelse och styra personuppgiftsansvarigas agerande i större utsträckning än under nu gällande dataskyddslagstiftning. Såsom närmare utvecklas i denna artikel menar vi att kraven i artikel 26 GDPR i de allra flesta fall bäst uppfylls genom ett s.k. datadelningsavtal.

1. INLEDNING

Den 25 maj 2018 ska GDPR börja tillämpas. Syftet med GDPR är bl.a. att skapa ett bättre och mer harmoniserat skydd för fysiska personers fri- och rättigheter vid behandling av deras personuppgifter.[3]

GDPR ersätter dataskyddsdirektivet[4] och personuppgiftslagen (1998:204) (PuL). Tidigare i år presenterade även Dataskyddsutredningen sitt betänkande[5] med ett förslag till ny svensk dataskyddslag med regler som ska komplettera GDPR.

De flesta av reglerna i såväl GDPR som dataskyddsdirektivet och PuL vänder sig till personuppgiftsansvarig. Att känna till vem eller vilka som är personuppgiftsansvarig för viss behandling av personuppgifter är således en förutsättning för att kunna uppfylla relevanta krav i dataskyddslagstiftningen.

I vår rådgivning har vi många gånger analyserat frågor om personuppgiftsansvarets fördelning när flera aktörer är inblandade i samma eller närliggande behandlingar av personuppgifter. I samband med det

1 Johan Kahn är advokat och delägare på Advokatfirman Kahn Pedersen. Fredrik Gustafsson är advokat och Senior Associate på samma byrå.

2 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

3 Beaktandesats 10 i GDPR.

4 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

5 SOU 2017:39 *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning*.

har även frågor kring avtalsreglering med anledning av artikel 26 GDPR hanterats.

I denna artikel kommer vi att redogöra för hur fastställande av personuppgiftsansvar för en viss personuppgiftsbehandling kan utföras. I samband med det kommer vi att presentera den schematiska modell för fördelning av personuppgiftsansvar som vi allt oftare tillämpat vid vår rådgivning.[6] Vi kommer även att kommentera behovet av avtalsreglering, såsom datadelningsavtal, beroende på personuppgiftsansvarets fördelning.

2. PERSONUPPGIFTSANSVAR – EN FRÅGA OM BESTÄMMANDERÄTT

Ett grundläggande krav i GDPR, dataskyddsdirektivet och PuL är att det måste klargöras vem eller vilka som är personuppgiftsansvarig för en viss behandling[7] av personuppgifter inom författningarnas tillämpningsområde[8].

Legaldefinitionen av personuppgiftsansvarig är i allt väsentligt densamma under dataskyddsdirektivet, PuL och GDPR.[9] I GDPR definieras ”personuppgiftsansvarig” enligt följande:

> ”[P]ersonuppgiftsansvarig: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter […]” (vår understrykning).[10]

Av legaldefinitionen följer att personuppgiftsansvaret kan bäras av en aktör ensamt eller av flera aktörer gemensamt. Om flera aktörer är inblandade i samma eller närliggande behandlingar av personuppgifter måste det utredas vilken eller vilka av dessa aktörer som är personuppgiftsansvarig för behandlingen, så att aktören eller aktörerna kan tillse att skyldigheterna under GDPR som åligger personuppgiftsansvarig uppfylls.

6 Se vidare avsnitt 3 nedan.

7 Med en behandling avses en åtgärd eller serie av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, t.ex. insamling, lagring, bearbetning eller ändring samt utlämning genom överföring, se vidare artikel 4 GDPR.

8 Författningarnas materiella tillämpningsområde framgår av artikel 2 GDPR, artikel 3 dataskyddsdirektivet samt 5 § PuL.

9 Se artikel 4 GDPR, artikel 2 dataskyddsdirektivet samt 3 § PuL. Märk väl att i artikel 3 dataskyddsdirektivet används uttrycket registeransvarig istället för personuppgiftsansvarig.

10 Artikel 4 GDPR.

En personuppgiftsansvarig har per definition alltid bestämmanderätt över ändamålen och medlen för behandlingen.[11] Motsatsvis innebär det att en aktör som *de facto* bestämmer över ändamål och medel inte kan vara personuppgiftsbiträde för den behandlingen.[12]

Med rätten att bestämma över ändamål och medel avses rätten att bestämma över varför respektive hur en behandling ska utföras. Viktiga omständigheter för att avgöra graden av bestämmande är varför behandlingen utförs och vem som är initiativtagare till behandlingen.[13] När det gäller rätten att bestämma över ändamål så är den aktör som har sådan bestämmanderätt alltid personuppgiftsansvarig för den behandlingen, antingen ensamt eller gemensamt med annan. Beslut om medel för behandlingen kan dock delegeras i fråga om tekniska och organisatoriska frågor.[14]

Delegation innebär att en aktör med viss bestämmanderätt över medlen inte nödvändigtvis är personuppgiftsansvarig, om bestämmanderätten har delegerats av en personuppgiftsansvarig, eller om bestämmanderätten grundar sig på krav som ställs på personuppgiftsbiträden enligt GDPR eller annan lagstiftning. Personuppgiftsansvarig lär dock inte kunna delegera beslut om medel i sådan utsträckning att denne inte längre kan utöva bestämmanderätt över dessa. I sådana fall lär det tilltänkta personuppgiftsbiträdet upphöra att vara biträde och istället bli ansvarig för den faktiska behandlingen, sannolikt tillsammans med den aktör som ursprungligen ansågs vara ensamt ansvarig för behandlingen.[15]

Vem eller vilka som har rätt att bestämma över en viss behandling avgörs av de faktiska omständigheterna i varje enskilt fall. Graden av självbestämmande och manöverutrymme i beslutsfattandet utgör viktiga parametrar för att avgöra

11 Artikel 4 GDPR. Se även artikel 2 dataskyddsdirektivet och 3 § PuL.

12 Detta följer redan av definitionen av personuppgiftsbiträde i artikel 4 GDPR: ”[…] en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning” (vår understrykning). Numera framgår detta även uttryckligen av artikel 28.10 GDPR.

13 Artikel 29-arbetsgruppen för skydd av personuppgifter, *Yttrande 1/2010 om begreppen registeransvarig och registerförare* s. 13. Artikel 29-gruppen är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet. Se även Datainspektionen dnr 686-2010, beslut 2010-07-02, samt Förvaltningsrätten i Stockholm, mål nr 9987-12, dom 2013-10-14. Se vidare Sören Öman och Hans-Olof Lindblom, *Personuppgiftslagen – En kommentar*, fjärde [rev.] upplagan, Norstedts Juridik, Stockholm, 2011 s. 93.

14 Artikel 29-gruppen, *Yttrande 1/2010* s. 14. Jfr artiklarna 28.3 c och 32 GDPR, artiklarna 17.2 och 17.3 dataskyddsdirektivet samt 30–31 §§ PuL.

15 Jfr artikel 28.10 GDPR.

bestämmanderätten.[16] Rätten att bestämma kan – uttryckt med de begrepp som Artikel 29-gruppen brukar och som vi för resonemangets skull har valt att använda – bero på (i) uttrycklig behörighet, (ii) underförstådd behörighet eller (iii) faktiskt inflytande.[17]

Med uttrycklig behörighet avses att bestämmanderätten framgår av lagtext eller är en direkt följd av lagtext. Myndighetsspecifika registerförfattningar är exempel på lagstiftning där personuppgiftsansvaret ofta framgår av lagtext. I andra fall, då det saknas bestämmelse om uttrycklig behörighet, kan en aktör ha en underförstådd behörighet att bestämma över ändamål och medel. Med underförstådd behörighet avses att behörigheten härrör ur rättsliga bestämmelser eller etablerad rättspraxis på området. Vissa roller får anses medföra en slags presumtion för personuppgiftsansvar: t.ex. arbetsgivare i förhållande till anställda, föreningar i förhållande till medlemmar och företag i förhållande till kunder. I dessa fall utgör rätten att bestämma en naturlig del av aktörens roll, och det är således rimligt att samma ansvarsfördelning ur ett dataskyddsperspektiv ska gälla även i förhållande till personuppgiftsbehandlingen, förutsatt att en sådan ordning återspeglar de faktiska omständigheterna.[18]

Graden av bestämmande kan även grunda sig på faktiskt inflytande över behandlingen. Av de tre kategorierna som avgör bestämmanderätt är denna ofta den svåraste att tillämpa. Utifrån avtal och annan dokumentation kring aktörernas förhållanden är det ofta möjligt att utläsa om en aktör har bestämmanderätt eller en dominerande roll med avseende på behandlingen. Förutsatt att en sådan ordning återspeglar de faktiska omständigheterna vid behandlingen finns det skäl att godta den som avgörande för graden av bestämmande. I tveksamma fall kan även den grad av verkligt personuppgiftsansvar som en aktör utövar, trots att detta inte framgår av avtal, tillsammans med de registrerades förmodade uppfattning i frågan samt de registrerades rimliga förväntningar påverka bedömningen.[19]

3. SCHEMATISK MODELL FÖR FÖRDELNING AV PERSONUPPGIFTSANSVAR

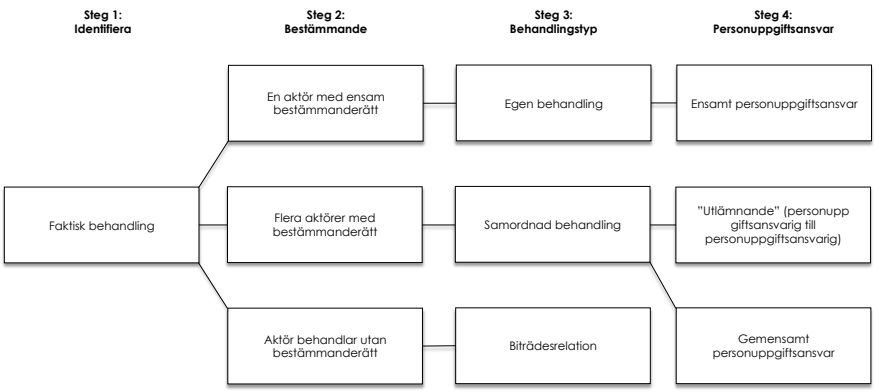
Artikel 29-gruppen har i sitt yttrande 1/2010 i förhållande till dataskyddsdirektivet närmare utrett förutsättningarna för fördelning av personuppgifts-

16 Artikel 29-gruppen, *Yttrande 1/2010* s. 13. Se vidare avsnitt 4.3 nedan om molntjänster.
17 Artikel 29-gruppen, *Yttrande 1/2010* s. 10–12.
18 Artikel 29-gruppen, *Yttrande 1/2010* s. 10.
19 Artikel 29-gruppen, *Yttrande 1/2010* s. 11–12.

ansvar. Yttrandet är formellt sett inte bindande. Mot bakgrund av Artikel 29-gruppens ställning och oberoende roll samt i avsaknad av vägledande praxis från Europeiska unionens domstol bör emellertid yttrandet utgöra det bästa tolkningsstödet i frågan.

Som nämnts ovan är legaldefinitionen av personuppgiftsansvar i allt väsentligt densamma under såväl PuL som dataskyddsdirektivet och GDPR. Detta talar för att bedömningen av fördelningen av personuppgiftsansvar under GDPR, utifrån dagens förutsättningar, bör utföras enligt samma principer som redan gäller under dataskyddsdirektivet och PuL. Av det följer att Artikel 29-gruppens yttrande 1/2010 alltjämt är aktuellt och relevant i förhållande till GDPR.

Utifrån Artikel 29-gruppens yttrande 1/2010 har vi utvecklat en enkel schematisk modell i syfte att underlätta bedömningen av fördelningen av personuppgiftsansvar. Modellen för fördelning av personuppgiftsansvar innehåller fyra steg, vilka närmare beskrivs nedan, och kan illustreras enligt följande:



I **steg 1** identifieras och kartläggs en viss faktisk behandling, dvs. en åtgärd eller en serie av åtgärder för samma ändamål.[20] För att kunna tillämpa modellen krävs därmed kunskap om: a) varför behandlingen utförs (ändamålet), b) vilka personuppgifter som behandlas och c) vilka aktörer som är inblandade.

20 Se definitionen av en behandling i artikel 4 GDPR samt i fotnot 7.

I **steg 2** utreds vilken eller vilka av de aktörer som har identifierats i steg 1 som bestämmer över ändamålen och medlen för den faktiska behandlingen. Bedömningen bör genomföras per aktör. Bestämmanderätten kan – med Artikel 29-gruppens terminologi – grundas på uttrycklig behörighet, underförstådd behörighet och/eller faktiskt inflytande. För det fall ingen av de aktörer som har identifierats i steg 1, mot förmodan, skulle anses ha sådan bestämmanderätt så måste steg 1 göras om, för att identifiera möjliga ytterligare aktörer. När det sker en behandling av personuppgifter i GDPR:s mening ska det nämligen alltid finnas åtminstone någon som är personuppgiftsansvarig.

I **steg 3** kategoriseras behandlingen enligt följande tre behandlingstyper: a) egen behandling, b) samordnad behandling och/eller c) biträdesrelation. Om behandlingen kategoriseras som en egen behandling, så är en aktör ensamt personuppgiftsansvarig för den behandlingen. Involverar behandlingen flera aktörer där endast en aktör har bestämmanderätt, så kategoriseras behandlingen som en biträdesrelation. Om behandlingen däremot involverar flera aktörer med bestämmanderätt kategoriseras detta som en samordnad behandling.

I **steg 4** fastställs och dokumenteras personuppgiftsansvaret för den faktiska behandlingen. Även bedömningen som personuppgiftsansvaret grundar sig på, dvs. steg 1 till 3, bör dokumenteras. Om den aktuella behandlingen utgör en samordnad behandling ska det klargöras om behandlingen utgör ett utlämnande från personuppgiftsansvarig till annan personuppgiftsansvarig eller om aktörerna är gemensamt personuppgiftsansvariga för behandlingen. Vid gemensamt personuppgiftsansvar och/eller en biträdesrelation, så finns det behov av avtalsreglering såsom inbördes arrangemang[21] och/eller personuppgiftsbiträdesavtal[22]. Vår uppfattning är emellertid att det även vid vissa former av utlämnande kan finnas behov av någon form av avtalsreglering.[23]

I anslutning till bedömningarna enligt ovan bör det prövas om fördelningen av personuppgiftsansvar är rimlig utifrån syftena med GDPR. Därvid ska särskilt beaktas om ansvarsfördelningen möjliggör för personuppgiftsansvarig och personuppgiftsbiträde att uppfylla sina respektive skyldigheter samt för de registrerade att utöva sina rättigheter enligt GDPR.[24] Om tillämpningen av modellen leder till onödig komplexitet eller andra oönskade konsekvenser lär

21 Artikel 26 GDPR.
22 Artikel 28 GDPR. Se även avsnitt 5 nedan.
23 Se avsnitt 5.1 nedan.
24 Jfr artikel 26 GDPR om krav på inbördes arrangemang vid gemensamt personuppgiftsansvar.

det finnas viss möjlighet att omfördela ansvar mellan de inblandade aktörerna, t.ex. genom olika avtalskonstruktioner.[25] En sådan omfördelning får såklart inte medföra ett kringgående av GDPR, och det upplägg som tillämpas måste alltjämt återspegla de faktiska omständigheterna.

4. FÖRDELNING AV PERSONUPPGIFTSANSVAR I PRAKTIKEN

4.1 DATAINSPEKTIONENS SYN PÅ PERSONUPPGIFTSANSVAR

Datainspektionen redovisar sällan, t.ex. i sin tillsynspraxis, på vilka grunder som en aktör har bestämmanderätt över viss behandling. Datainspektionen uttalar sig inte heller särskilt ofta om huruvida aktören är ensamt personuppgiftsansvarig eller om flera aktörer kan vara gemensamt personuppgiftsansvariga för samma behandling.

En viktig utgångspunkt för Datainspektionen synes vara att någon aktör är personuppgiftsansvarig för en viss behandling och att fördelningen av personuppgiftsansvar ter sig rimlig och ändamålsenlig.[26] Detta är naturligtvis en bra utgångspunkt men som framgår av denna artikel kan det ofta vara en svår uppgift att avgöra vem som är personuppgiftsansvarig för samma eller närliggande behandlingar. Detta gäller särskilt i koncerner och andra stora komplexa organisationer. Ytterligare vägledning från Datainspektionen kring fördelning av personuppgiftsansvar vore därför önskvärt.

4.2 NÅGRA ILLUSTRATIVA EXEMPEL

Nedan följer några illustrativa exempel på hur några myndigheter och domstolar har bedömt att personuppgiftsansvaret fördelar sig.

Datainspektionen har uttalat att myndigheter bör vara personuppgiftsansvarig för den behandling av personuppgifter som sker inom den egna verksamheten.[27] Om en myndighet beordrar viss behandling av personuppgifter hos ett bolag, såsom i samband med tillsyn, bör myndigheten vara personuppgiftsansvarig även för sådan behandling.[28]

25 Jfr Artikel 29-gruppens *Yttrande 1/2010* s. 23 samt liknande resonemang på s. 7 och 19. Se därutöver SOU 2015:39 *Myndighetsdatalag* s. 343–344.

26 Jfr *Samrådsyttrande om fördelning av personuppgiftsansvar – E-delegationsprojektet Effektiv informationsförsörjning*, dnr 195-2014, beslut 2014-03-18, där Datainspektionen emellertid relativt utförligt redogör för däri tillämpade bedömningsgrunder.

27 Datainspektionens informationsblad, *E-förvaltning och personuppgiftslagen – Statliga myndigheters behandling av personuppgifter*.

28 Prop. 1998/99:34 *Behandling av personuppgifter i skattemyndigheternas brottsutredande verksamhet m.m.* s. 67 ff., SOU 1999:105 *Skatt – Tull – Exekution – Normer för behandling av personuppgifter* s. 369 ff. och prop. 2000/01:33 *Behandling av personuppgifter inom skatt, tull och*

Datainspektionen har uttalat att arbetsgivare normalt sett är personuppgiftsansvarig för behandling av uppgifter rörande sina anställda.[29]

Datainspektionen har uttalat att både kommunstyrelsen och de kommunala nämnderna – förutsatt att de är så självständiga att de är förvaltningsmyndigheter – var för sig bör anses som personuppgiftsansvarig i sin verksamhet.[30]

Datainspektionen har uttalat att vid behandling av elevers personuppgifter i skolor som bedrivs i kommunal regi bör ofta den kommunala myndigheten vara personuppgiftsansvarig.[31]

Datainspektionen har uttalat att den som använder molntjänster är personuppgiftsansvarig och att molntjänstleverantören är personuppgiftsbiträde.[32]

Europeiska unionens domstol har ansett att en söktjänstleverantör är personuppgiftsansvarig för den behandling av personuppgifter som sker när denne sammanställer sökresultat utifrån information som tredje män gjort tillgänglig på internet.[33]

Högsta förvaltningsdomstolen har i ett avgörande ansett att när Försäkringskassan tillhandahåller en SMS-tjänst, så är myndigheten personuppgiftsansvarig inte enbart för själva tjänsten utan även för den behandling som sker innan personuppgifterna blir tillgängliga för Försäkringskassan. Detta eftersom de åtgärder som vidtas med personuppgifterna innan de blir tillgängliga kan betraktas som ett led i Försäkringskassans behandling av uppgifter i enskilda ärenden.[34]

4.3 SÄRSKILT OM MOLNTJÄNSTER

Vi menar att frågan om i vilken utsträckning som en personuppgiftsansvarig kan delegera bestämmanderätt över medel för personuppgiftsbehandlingen är särskilt intressant i förhållande till användning av standardiserade publika

exekution s. 137–138.

29 Datainspektionens informationsblad, *Personuppgifter i arbetslivet*.

30 Datainspektionens informationsblad, *Personuppgiftsansvar*.

31 Datainspektionens rapport 2002:2, *Behandling av elevers personuppgifter i grundskolan*.

32 Datainspektionens informationsblad, *Molntjänster och personuppgiftslagen*. Se vidare avsnitt 4.3 nedan.

33 EU-domstolen, dom av den 13 maj 2014 (*Google Spain*), C-131/12.

34 HFD 2012 ref. 21. Se vidare Daniel Westman, *Personuppgiftsansvarets gränser*, Lov&Data nr 111, 2012.

molntjänster.[35] Detta då leverantörer av sådana tjänster i stor utsträckning – för att inte säga ensamt – kan bestämma över medlen för behandlingen, dvs. hur behandlingen ska utföras.

Datainspektionens syn på molntjänster får uppfattas som att den som använder molntjänsten ”alltid” är personuppgiftsansvarig och att molntjänstleverantören är personuppgiftsbiträde.[36] Enligt vår erfarenhet delas denna uppfattning av såväl kunder som leverantörer, i vart fall i Sverige. Vissa utländska leverantörer synes ha en motsatt uppfattning och anser sig vara personuppgiftsansvarig för i stort sett alla personuppgifter som de behandlar. Vår uppfattning är att det kan finnas skäl att ifrågasätta eller åtminstone nyansera dessa ståndpunkter.

Om molntjänstkunden varken har uttrycklig behörighet, underförstådd behörighet eller faktiskt inflytande över den behandling som molntjänstleverantören utför kan molntjänstkunden å ena sidan inte rimligen anses vara ensamt personuppgiftsansvarig. Å andra sidan måste en molntjänstkund i normalfallet anses ha bestämmanderätt baserat på exempelvis underförstådd behörighet (t.ex. i rollen som arbetsgivare), en bestämmanderätt som inte rimligen kan anses upphöra när uppgifterna behandlas av molntjänstleverantören.

Den franska dataskyddsmyndigheten (CNIL) har uttryckt en liknande uppfattning i frågan och anser att molntjänstkunden i vissa fall, och för vissa behandlingar, kan vara gemensamt personuppgiftsansvarig för behandlingen i fråga tillsammans med molntjänstleverantören. Enligt CNIL beror det på att molntjänstleverantörer ofta erbjuder högt standardiserade tjänster till standardiserade villkor, dvs. tjänster som inte är anpassade till enskilda molntjänstkunder och regleras av villkor som inte kan förhandlas.[37] Såvitt vi känner till saknas dock vägledande praxis som talar för en sådan uppdelning av ansvar. Sådan uppdelning har, enligt vår erfarenhet, heller inte godtagits inom branschen.

Om molntjänstkund och molntjänstleverantör bedöms vara gemensamt personuppgiftsansvariga för vissa behandlingar, t.ex. lagring, är kravet på ett inbördes arrangemang tillämpligt.[38] Det skulle i sin tur innebära att molntjänstkunden och molntjänstleverantören behöver teckna personuppgiftsbiträdesavtal och, såvitt avser sådan del i molntjänsten som innebär gemensamt personuppgiftsansvar, ingå ett inbördes arrangemang enligt artikel 26 GDPR.

35 Se vidare avsnitt 2 ovan.
36 Se Datainspektionens informationsblad, *Molntjänster och personuppgiftslagen*.
37 CNIL, *Recommendations for companies planning to use Cloud computing services* s. 5–6.
38 Artikel 26 GDPR.

5. ANSVARSFÖRDELNING OCH BEHOV AV AVTALSREGLERING

5.1 SAMORDNADE BEHANDLINGAR

Om två eller flera aktörer har bestämmanderätt över en viss behandling ska det, med tillämpning av den modell som redogörs för ovan, anses utgöra en samordnad behandling.

I huvudsak kan personuppgiftsansvar i samband med samordnade behandlingar beskrivas på följande två sätt:

a) gemensamt personuppgiftsansvar, eller

b) utlämnande från personuppgiftsansvarig till annan personuppgiftsansvarig.

Av artikel 26 framgår att gemensamt personuppgiftsansvariga ”under öppna former ska fastställa sitt respektive ansvar för att fullgöra skyldigheterna” enligt GDPR genom ett inbördes arrangemang. Arrangemanget ska särskilt avse former och ansvar för utövande av den registrerades rättigheter och skyldigheten att lämna information till registrerade. Vidare gäller att arrangemanget ”på lämpligt sätt ska återspegla gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade” samt att ”det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade”. Kravet på inbördes arrangemang är belagt med administrativ sanktionsavgift.[39]

Om en samordnad behandling istället beskrivs som ett utlämnande från en personuppgiftsansvarig till en annan personuppgiftsansvarig står det klart att den aktör som samlar in och initialt lagrar personuppgifterna är ansvarig för dessa behandlingar. Vidare är den aktör som mottar uppgifterna ansvarig för alla behandlingar som denne utför efter överföringen. Vad gäller ansvaret för själva överföringen (vilket är en behandling i sig) är situationen mer komplicerad. I vissa fall lär utlämnande och mottagande aktör vara gemensamt personuppgiftsansvariga för själva överföringen, förutsatt att de tillsammans bestämmer ändamål och medel för denna. Ett exempel på en sådan fördelning kan vara utlämnande inom ramen för gemensamma databaser eller system. Om utlämnande och mottagande aktör därvid bedöms vara gemensamt personuppgiftsansvariga för överföringen är kravet på ett inbördes arrangemang i artikel 26 GDPR tillämpligt. I andra fall lär endast en av aktörerna utöva bestämmanderätt över ändamål och medel för

39 Artikel 83.4 a GDPR.

överföringen. Så kan t.ex. vara fallet när en myndighet (t.ex. Skatteverket) bestämmer att ett bolag ska lämna ut vissa personuppgifter. I sådana fall är inte kravet på ett inbördes arrangemang tillämpligt.

Som ovan framgått krävs ett inbördes arrangemang för det fall flera aktörer är gemensamt personuppgiftsansvariga. Kravet på ett arrangemang innebär inte ett uttryckligt krav på avtal aktörerna sinsemellan. Enligt vår bedömning är det dock klart att ett sådant arrangemang bör dokumenteras och regleras inom ramen för ett skriftligt avtal. Innehållet i det inbördes arrangemanget måste anpassas till de rådande omständigheterna. I vissa fall kan det vara tillräckligt att reglera samverkan/datautbytet i ett tjänsteavtal mellan parterna vars uppfyllande medför personuppgiftsbehandling. I andra fall kan det vara lämpligt med ett fristående och mera omfattande datadelningsavtal.

Några exempel på områden som ofta behöver regleras är: (i) de olika aktörerna och deras roller, (ii) varför data delas (ändamålet), (iii) vilken typ av data som ska/får delas, (iv) hur de registrerade kan utöva sina rättigheter, (v) hur de registrerade ska få tillräcklig information om behandlingen, (vi) hur de grundläggande principerna för behandling av personuppgifter uppfylls, (vii) laglig grund för datadelning och (viii) om någon av de ansvariga ska utgöra en gemensam kontaktpunkt för de registrerade.[40] Andra viktiga frågor är gallring, säkerhet i behandlingen, konfidentialitet och möjligheterna till kontroll av den andre partens avtalsefterlevnad. Som ovan nämnts ska de gemensamt personuppgiftsansvariga se till att det väsentliga innehållet i arrangemanget, i detta fall datadelningsavtalet, görs tillgängligt för de registrerade.[41]

Utöver vad som ovan anförts är det vår uppfattning att personuppgiftsansvarig bör överväga om någon form av arrangemang kan vara lämpligt även i de fall av utlämnanden där en av aktörerna ensamt bestämmer över ändamål och medel för överföringen, dvs. utanför tillämpningsområdet för artikel 26 GDPR. Behovet av ett sådant arrangemang får såklart bedömas från fall till fall och utifrån aktuella omständigheter. Normalt sett bör den utlämnande aktören i vart fall försäkra sig om att personuppgifterna inte behandlas i strid med GDPR av den mottagande aktören. Den mottagande aktören bör i sin tur i vart fall försäkra sig om att de registrerade fått korrekt information om utlämnandet och att insamlandet i övrigt var lagligt. Detta kan i förlängningen innebära ett behov av koordinerad hantering av registrerades utövande av sina rättigheter, informationslämning,

40 Jfr ICO, *Data sharing code of practice*, 2011, se särskilt s. 41–43.
41 Artikel 26.2 GDPR.

reglering avseende säkerhetsåtgärder osv. Skillnaden jämfört med ett inbördes arrangemang enligt artikel 26 GDPR förefaller därmed inte som särskilt stor.

5.2 PERSONUPPGIFTSBITRÄDESRELATION

Om en personuppgiftsbiträdesrelation identifieras ska personuppgiftsansvarig ingå ett skriftligt personuppgiftsbiträdesavtal med biträdet i fråga.[42] Kravet på skriftlighet finns även i dataskyddsdirektivet och PuL.[43]

De uttryckliga lagkraven på innehållet i personuppgiftsbiträdesavtal skiljer sig något vid en jämförelse mellan å ena sidan PuL och dataskyddsdirektivet och å andra sidan GDPR. Vid en första anblick kan det därmed förefalla som om GDPR medför en lång rad helt nya krav på innehållet i ett biträdesavtal. GDPR är dock i vissa delar en kodifiering av den praxis och sedvänja som utvecklats inom EU de senaste åren. I Sverige har utvecklingen avseende innehåll i biträdesavtal framförallt drivits av Datainspektionens tillsyn avseende molntjänster, vilken utmynnat i flera tillsynsbeslut och allmänna regler för vad ett biträdesavtal ska innehålla för att möta kraven i PuL och dataskyddsdirektivet.[44]

Exempel på redan gällande krav på personuppgiftsbiträdesavtal enligt Datainspektionens beslut i ovannämnda tillsynsärenden är:

- Att personuppgiftsansvarig ska kunna utföra kontroll av biträdets, och eventuella underbiträdens, behandling av personuppgifter.[45]

- Att biträden på den personuppgiftsansvariges anmodan och vid behandlingens upphörande antingen ska radera eller återlämna de behandlade personuppgifterna.[46]

- Att ett biträde kan ges mandat att ingå biträdesavtal för den ansvariges räkning om biträdet anlitar ett underbiträde, under förutsättning

42 Artikel 28 GDPR.

43 Artikel 17 dataskyddsdirektivet och 30 § PuL.

44 Datainspektionen, dnr 263-2011, beslut 2011-09-28 (*Salems kommun*). Detta beslut följdes senare upp av Datainspektionen, dnr 1351-2012, beslut 2013-05-31; Förvaltningsrätten i Stockholm, dom 2014-07-01, mål nr 15410-13; Datainspektionen, dnr 574-2011, beslut 2011-09-28 (*Brevo*); och Datainspektionen, dnr 256-2011, 2011-09-28 (*Enköpings kommun*). Se även en sammanfattning av Datainspektionens uttalanden rörande molntjänster i Datainspektionens informationsblad, *Molntjänster och personuppgiftslagen*.

45 Jfr artikel 28.3 h GDPR.

46 Jfr artikel 28.3 g GDPR.

> att biträdets avtal med underbiträdet ska innehålla krav som motsvarar personuppgiftsbiträdesavtalet mellan personuppgiftsansvarig och biträdet.[47]

På ett mer principiellt plan innebär GDPR att personuppgiftsbiträdets roll förändras på så vis att biträden får nya skyldigheter och, som Datainspektionen uttrycker det, utökat eget ansvar för behandlingar.[48] Som exempel kan biträden under GDPR bli skyldiga att betala en administrativ sanktionsavgift och bli skadeståndsskyldiga gentemot de registrerade.[49] Motsvarande bestämmelser i PuL om förbud vid vite och skadestånd gäller endast för personuppgiftsansvarig.[50]

Det utökade ansvaret för personuppgiftsbiträden i GDPR kan vidare exemplifieras genom att GDPR medför ett eget ansvar för biträden att vidta säkerhetsåtgärder, underrätta personuppgiftsansvarig vid en personuppgiftsincident, i vissa fall föra register över de behandlingar som biträdet utför samt i vissa fall utse ett dataskyddsombud.[51] Personuppgiftsbiträden ska därutöver informera personuppgiftsansvarig om biträdet anser att den ansvariges instruktioner strider mot GDPR eller annan dataskyddsbestämmelse, och är i allmänhet skyldig att bistå den ansvarige när denne ska fullgöra sina skyldigheter enligt GDPR.[52] GDPR innebär således att ansvarsfördelningen mellan personuppgiftsansvarig och personuppgiftsbiträden förskjuts, så att biträden får ett större ansvar för behandlingen och för uppfyllande av lagstiftningen. Detta är betydelsefulla förändringar som bör återspeglas i personuppgiftsbiträdesavtalet.

6. AVSLUTANDE KOMMENTARER

Den omständigheten att GDPR innehåller särskilda bestämmelser för reglering av det gemensamma personuppgiftsansvaret får ses som en anpassning till verkligheten snarare än en förändring av de grundläggande förutsättningarna för bestämmande av personuppgiftsansvarets fördelning. Det är förmodligen så att många behandlingar som ansetts ha en personuppgiftsansvarig under PuL och dataskyddsdirektivet kan komma att behöva omprövas och anpassas till den mer nyanserade och enskilda bedömning som måste göras i enlighet med GDPR. Därmed är vår uppfattning att det gemen-

47 Jfr artikel 28.2 och 28.4 GDPR.
48 Se Datainspektionens informationsblad, *Vägledning för personuppgiftsbiträden*.
49 Artikel 82–83 GDPR.
50 45 och 48 §§ PuL.
51 Artiklarna 32, 33.2, 30.2 och 37 GDPR.
52 Artikel 28.3 GDPR.

samma personuppgiftsansvaret kommer att få större betydelse och styra personuppgiftsansvarigas agerande i större utsträckning under GDPR än under PuL och dataskyddsdirektivet.

Det krav på inbördes arrangemang som GDPR ställer för hantering av gemensamt personuppgiftsansvar bör i de allra flesta fall bäst uppfyllas genom ingående av datadelningsavtal. Ett avtal som på ett tydligt sätt ålägger gemensamt personuppgiftsansvariga skyldigheter vad gäller de registrerades utövande av sina rättigheter samt informationsgivning under GDPR borde vara den typ av inbördes arrangemang som tydligast uppfyller GDPR:s krav. Datadelningsavtalet kan även med fördel hantera de risker och övriga affärsmässiga aspekter som följer av ett gemensamt personuppgiftsansvar, såsom formerna för parternas samverkan.

Datadelningsavtalet måste enligt vår uppfattning, i syfte att personuppgiftsansvaret ska vara intakt, föreskriva enhällighet kring beslut som berör den gemensamma personuppgiftsbehandlingen. Beslutsordningar som bygger på majoritetsbeslut innebär att minoriteten inte längre bestämmer över ändamålen och medlen för den aktuella personuppgiftsbehandlingen och således inte kan definieras som personuppgiftsansvariga. Dessa aktörer, som berövats sin bestämmanderätt, blir då antingen självständigt personuppgiftsansvariga efter utlämnande av aktuella personuppgifter från majoriteten, alternativt personuppgiftsbiträden eller – om de inte längre behandlar aktuella personuppgifter – ingenting i GDPR:s mening.